Lecture Notes in Computer Science 2052
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Vladimir I. Gorodetski Victor A. Skormin
Leonard J. Popyack (Eds.)

Information Assurance in Computer Networks

Methods, Models and Architectures for Network Security

International Workshop MMM-ACNS 2001
St. Petersburg, Russia, May 21-23, 2001
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Vladimir I. Gorodetski
St. Petersburg Institute for Informatics
and Automation of the Russian Academy of Sciences (SPIIRAS)
SPIIRAS, 39, 14th Liniya, St. Petersburg, Russia 199178
E-mail: gor@mail.iias.spb.su

Victor A. Skormin
Binghamton University, Watson School of Engineering
Binghamton, NY 13902, USA
E-mail: vskormin@binghamton.edu

Leonard J. Popyack
Air Force Research Laboratory
Defensive Information Warfare Branch
525 Brooks Road, Rome, NY 13441-4505
E-mail: Leonard.Popyack@rl.af.mil

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information assurance in computer networks : methods, models, and
architectures for network security ; proceedings / International
Workshop MMM ACNS 2001, St. Petersburg, Russia, May 21 - 23, 2001.
Vladimir I. Gorodetski ... (ed.). - Berlin ; Heidelberg ; New York ;
Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo :
Springer, 2001
(Lecture notes in computer science ; 2052)
ISBN 3-540-42103-3

CR Subject Classification (1998): C.2, D.4.6, E.3, K.6.5, K.4.1, K.4.4, J.1

ISSN 0302-9743
ISBN 3-540-42103-3 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by PTP Berlin, Stefan Sossna
Printed on acid-free paper SPIN 10781519 06/3142 5 4 3 2 1 0

Preface

This volume contains the papers selected for presentation at the International Workshop on Mathematical Methods, Models and Architectures for Network Security Systems (MMM-ACNS 2001) held in St. Petersburg, Russia, May 21–23, 2001. The workshop was organized by the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in cooperation with the Russian Foundation for Basic Research (RFBR), the US Air Force Research Laboratory (both the Information Directorate (AFRL/IF)) and the Office of Scientific Research (AFRL/OSR), and Binghamton University (USA).

MMM-ACNS 2001 provided an international forum for sharing original research results and application experiences among specialists in fundamental and applied problems of computer network security. An important distinction of the workshop was its focus on mathematical aspects of information and computer network security and the role of mathematical issues in contemporary and future development of models of secure computing.

A total of 36 papers coming from 12 different countries on significant aspects of both theory and applications of computer network and information security were submitted to MMM-ACNS 2001. Out of them 24 were selected for regular presentation. Five technical sessions were organized, namely: mathematical models for computer networks and applied systems security; methods and models for intrusion detection; mathematical basis and applied techniques of cryptography and steganography; applied techniques of cryptography; and models for access control, authentication, and authorization. Two panel discussions were devoted to the significant issues in the computer and information security field. The first sought to define the important open problems in computer security and to reach a conclusion as to mathematical methods and models can contribute, and the second focused upon security research and education in academia. The MMM-ACNS 2001 program was enriched by five invited speakers: Dipankar Dasgupta, Alexander Grusho, Catherine Meadows, Ravi Sandhu, and Vijay Varadharajan.

An event like this can only succeed as a result of team efforts. We would like to acknowledge the contribution of the Program Committee members and thank the reviewers for their efforts. Our sincere gratitude goes to all of the authors who submitted papers.

We are grateful to our sponsors: the European Office of Aerospace Research and Development (EOARD), the European Office of Naval Research International Field Office (ONRIFO), and the Russian Foundation of Basic Research (RFBR) for their generous support.

We wish to express our thanks to Alfred Hofmann of Springer-Verlag for his help and cooperation.

May 2001

Vladimir Gorodetski
Leonard Popyack
Victor Skormin

MMM-ACNS 2001 Workshop Committee

General Chairmen:

Victor Skormin	Watson School of Eng., Binghamton Univ., USA
Rafael Yusupov	St. Petersburg Inst. for Informatics and Automation, Russia

International Organizing Committee

Barry Mckiney	Air Force Research Laboratory/IF, USA
Michael Morgan	Office of Naval Research Int. Field Office, USA
Christopher Reuter	European Office of Aerospace R&D, USA
Rafael Yusupov	St. Petersburg Inst. for Informatics and Automation, Russia

Program Committee

Program Co-chairmen:

Vladimir Gorodetski	St. Petersburg Inst. for Informatics and Automation, Russia
Leonard Popyack	Air Force Research Laboratory/IF, USA
Victor Skormin	Watson School of Eng., Binghamton Univ., USA

International Program Committee

Kurt Bauknecht	Univ. of Zurich, Dept. of Information Technology, Switzerland
Harold Carter	University of Cincinnati, USA
Peter Chen	Computer Science Dept., Luisiana State Univ., USA
Dipankar Dasgupta	Div. of Computer Science, Univ. of Memphis, USA
Jose G. Delgado-Frias	Electrical and Comp. Eng. Dept., Univ. of Virginia, USA
Lynette Drevin	Comp. Science and Inf. Systems, Potchefstroom Univ., South Africa
Jiri Fridrich	Watson School of Eng., Binghamton Univ., USA
Dimitris Gritzalis	Athens Univ. of Economics & Business, Greece
Alexander Grusho	Russian State Univ. for Humanity, Russia
Yury Karpov	St. Petersburg State Technical Univ., Russia
Igor Kotenko	St. Petersburg Inst. for Informatics and Automation, Russia
Martin Kutter	AlpVision, Les Paccots, Switzerland
Anatoly Maliuk	Moscow State Engineering Physical Inst., Russia
Catherine Meadows	Naval Research Laboratory, USA
Nikolay Moldovian	Spec. Center of Program Systems "SPECTR", Russia
Vladimir Orlov	Microtest Company, Moscow, Russia
Gyorgy Papp	V.R.A.M. Communication Ltd., Hungary
Hartmut Pohl	Fachhochschule Bonn-Rhein-Sieg, St. Augustin-Univ. of Applied Sciences, Germany
Ravi Sandhu	SingleSignOn.Net Inc. and George Mason Univ., USA
Igor Sokolov	Inst. for Informatics Problems, Moscow, Russia
Mikhail Sycheov	Bauman State Technical Univ., Russia
Leonid Ukhlinov	The State Customs Committee of Russia, Russia
Vijay Varadharajan	Div. of Inf. and Commun. Sciences Macquarie Univ., Australia
Minerva M. Yeung	Media and Internet Technology, Intel, USA
Louise Yngstrom	Dept. of Comp. and Systems Sciences, Univ. & Royal Inst. of Technology, Stockholm
Peter Zegzhda	St. Petersburg State Technical Univ., Russia

Reviewers

Kurt Bauknecht	Univ. of Zurich, Dept. of Information Technology, Switzerland
Kirill Bolshakov	St. Petersburg State Technical Univ., Russia
Dipankar Dasgupta	Div. of Comp. Science, Univ. of Memphis, USA
Gunther Drevin	Comp. Science and Inf. Systems, Potchefstroom Univ., South Africa
Lynette Drevin	Comp. Science and Inf. Systems, Potchefstroom Univ., South Africa
Dimitris Gritzalis	Athens Univ. of Economics & Business, Greece
Vladimir Gorodetski	St. Petersburg Inst. for Informatics and Automation, Russia
Yury Karpov	St. Petersburg State Technical Univ., Russia
Igor Kotenko	St. Petersburg Inst. for Informatics and Automation, Russia
Evgenii Krouk	St. Petersburg State Technical Univ., Russia
Catherine Meadows	Naval Research Laboratory, USA
Nikolay Moldovian	Spec. Center of Program Systems "SPECTR", Russia
Gyorgy Papp	V.R.A.M. Communication Ltd., Hungary
Vladimir Platonov	St. Petersburg State Technical Univ., Russia
Alexander Rostovtsev	St. Petersburg State Technical Univ., Russia
Ravi Sandhu	SingleSignOn.Net Inc. and George Mason University, USA
Michael Smirnow	GMD, FOKUS, Germany
Igor Sokolov	Inst. for Informatics Problems, Moscow, Russia
Vijay Varadharajan	Div. of Inf. and Commun. Sciences, Macquarie Univ., Australia
Dmitry Zegzhda	St. Petersburg State Technical Univ., Russia
Peter Zegzhda	St. Petersburg State Technical Univ., Russia

Table of Contents

Intrusion Detection: Foundations and Models

Access Control, Authentication, and Authorization

Cryptography and Steganography: Mathematical Basis, Protocols, and Applied Methods